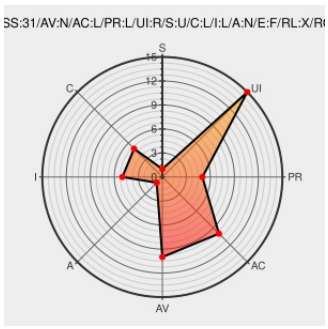
CVE-2021-43080

Published on: Not Yet Published

Last Modified on: 09/08/2022 08:39:00 PM UTC

CVE-2021-43080

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fortios from Fortinet contain the following vulnerability:

An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS version 7.2.0, version 6.4.0 through 6.4.9, version 7.0.0 through 7.0.5 may allow an authenticated attacker to perform a stored cross site scripting (XSS) attack through the URI parameter via the Threat Feed IP address section of the Security Fabric External connectors.

CVE-2021-43080 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **FortiOS 7.2.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
PSIRT Advisories | FortiGuard	fortiguard.com text/html	CONFIRM fortiguard.com/psirt/FG-IR-21-222

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

43934 FortiOS - Cross-Site Scripting (XSS) Vulnerability in External Connectors of Security Fabric (FG-IR-21-222)

Exploit/POC from Github

An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS version 7.2.0, versi…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	7.2.0	All	All	All

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:7.2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43080 : An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS v… twitter.com/i/web/status/1…	2022-09-06 15:55:30
/r/netcve	CVE-2021-43080	2022-09-06 16:38:50

← Previous ID

Next ID→